

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-111729  
 (43)Date of publication of application : 12.04.2002

(51)Int.CI. H04L 12/56  
 H04L 12/24  
 H04L 12/26

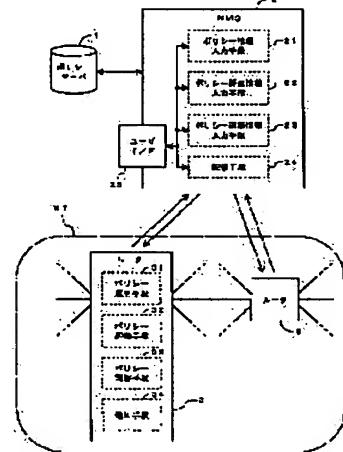
(21)Application number : 2000-300817 (71)Applicant : KDDI CORP  
 (22)Date of filing : 29.09.2000 (72)Inventor : YOSHIHARA TAKAHITO  
 HORIUCHI HIRONORI

## (54) APPARATUS FOR MANAGING POLICY BASE MANAGING SYSTEM AND APPARATUS TO BE MANAGED

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a policy base managing system capable of optimally regulating a policy to be operated in each router (apparatus to be managed) in a network real time in response to the state of traffic.

**SOLUTION:** The apparatus 3 to be managed in the network NT comprises a policy operating means 31 for operating policy information delivered from the apparatus 2 for managing the policy base managing system to control the traffic, a policy evaluating means 32 for evaluating the policy during operating based on policy evaluation information delivered from the apparatus 2, and a policy evaluating means 33 for dynamically regulating the policy during the operation based on the policy regulating information delivered from the apparatus 2 and the evaluation result by the evaluating means.



### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2002-111729

(P2002-111729A)

(43)公開日 平成14年4月12日(2002.4.12)

(51)Int.Cl.  
H04L 12/56  
12/24  
12/26

識別記号

F I  
H04L 11/20  
11/08

102 A 5K030

マークコード (参考)

審査請求 未請求 請求項の数11 O L (全11頁)

(21)出願番号 特願2000-300817(P2000-300817)

(22)出願日 平成12年9月29日(2000.9.29)

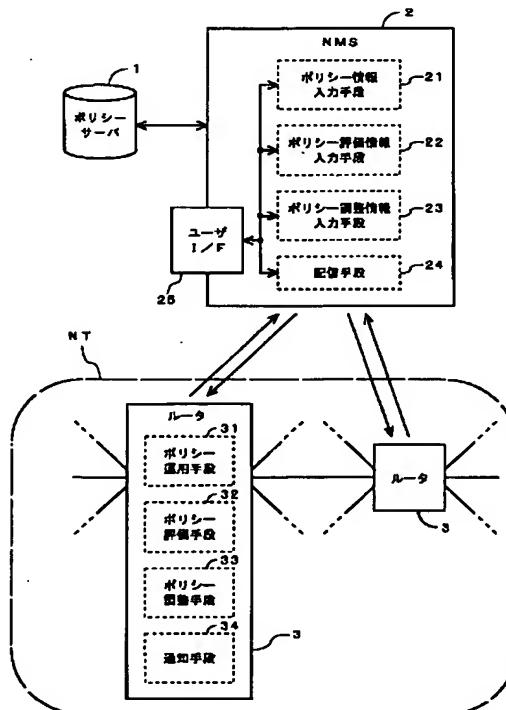
(71)出願人 000208891  
ケイディーディーアイ株式会社  
東京都新宿区西新宿二丁目3番2号  
(72)発明者 吉原 貴仁  
埼玉県上福岡市大原2-1-15 株式会社  
ケイディディ研究所内  
(72)発明者 堀内 浩規  
埼玉県上福岡市大原2-1-15 株式会社  
ケイディディ研究所内  
(74)代理人 100084870  
弁理士 田中 香樹 (外1名)  
Fターム(参考) 5K030 GA08 GA14 HB06 HB08 JA10  
KA01 KA07 LC09 LE17 MA04  
MB04 MC09

(54)【発明の名称】ポリシーベース管理システムの管理装置および被管理装置

(57)【要約】

【課題】 ネットワーク内の各ルータ(被管理装置)で運用されているポリシーを、トラヒックの状況に応じて実時間で最適に調整できるようにしたポリシーベース管理システムを提供する。

【解決手段】 ネットワークNT内の被管理装置3に、管理装置2から配信されたポリシー情報運用手段31と、管理装置2から配信されたポリシー評価情報に基づいて、運用中のポリシーを評価するポリシー評価手段32と、管理装置2から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを動的に調整するポリシー調整手段33とを設けた。



## 【特許請求の範囲】

【請求項1】 ポリシー情報を管理装置で一元管理し、当該ポリシー情報を被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの管理装置において、

ポリシー情報を入力するポリシー情報入力手段と、前記被管理装置においてポリシーの適用効果を評価させるための評価情報を入力するポリシー評価情報入力手段と、

前記被管理装置で運用されるポリシーを、前記評価結果に基づいて被管理装置において動的に調整させるための調整情報を入力するポリシー調整情報入力手段と、

前記入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報を前記被管理装置へ配信する配信手段とを含むことを特徴とするポリシーベース管理システムの管理装置。

【請求項2】 前記ポリシー評価情報は、各トラヒックに割り当てられたポリシーが当該トラヒックに適合しているか否かを判断させる情報を含み、

前記ポリシー調整情報は、不適合と判定されたポリシーを前記トラヒックに適合させる情報を含むことを特徴とする請求項1に記載のポリシーベース管理システムの管理装置。

【請求項3】 前記ポリシー評価情報は、運用中のポリシーが実際のトラヒックに対して資源不足であるか否かを判断させるための情報を含み、

前記ポリシー調整情報は、ポリシーの資源不足を緩和させるための情報を含むことを特徴とする請求項2に記載のポリシーベース管理システムの管理装置。

【請求項4】 前記ポリシー評価情報は、運用中のポリシーが実際のトラヒックに対して資源過剰であるか否かを判断させるための情報を含み、

前記ポリシー調整情報は、ポリシーの資源過剰を緩和させるための情報を含むことを特徴とする請求項2または3に記載のポリシーベース管理システムの管理装置。

【請求項5】 ポリシー情報を管理装置で一元管理し、当該ポリシー情報を被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの被管理装置において、

前記管理装置から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段と、

前記管理装置から配信されたポリシー評価情報に基づいて、運用中のポリシーを評価するポリシー評価手段と、前記管理装置から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを動的に調整するポリシー調整手段とを含むことを特徴とするポリシーベース管理システムの被管理装置。

【請求項6】 前記ポリシー評価手段は、各トラヒックに割り当てられたポリシーが当該トラヒックに適合しているか否かを評価し、

10 前記ポリシー調整手段は、前記評価手段に基づいてポリシーをトラヒックに適合させることを特徴とする請求項5に記載のポリシーベース管理システムの被管理装置。

【請求項7】 前記ポリシー調整手段は、前記評価手段により資源過剰と評価されたポリシーの品質を低下させることを特徴とする請求項6に記載のポリシーベース管理システムの被管理装置。

【請求項8】 前記ポリシー調整手段は、前記評価手段により資源不足と評価されたポリシーの品質を向上させることを特徴とする請求項6または7に記載のポリシーベース管理システムの被管理装置。

【請求項9】 前記ポリシー調整手段は、前記評価手段による評価結果に基づいて、各トラヒックに予め割り当てられているポリシーを調整することを特徴とする請求項5ないし8のいずれかに記載のポリシーベース管理システムの被管理装置。

【請求項10】 前記調整後のポリシー情報を管理装置および他の被管理装置の少なくとも一方へ通知する通知手段をさらに具備したことを特徴とする請求項5ないし9のいずれかに記載のポリシーベース管理システムの被管理装置。

【請求項11】 前記ポリシー調整手段は、他の被管理装置からの通知に基づいてポリシーを調整することを特徴とする請求項5ないし10のいずれかに記載のポリシーベース管理システムの被管理装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、ポリシー情報を管理装置で一元管理し、当該ポリシー情報をネットワーク30内の被管理装置へ配信してトラフィックを制御するポリシーベース管理システムの管理装置および被管理装置に係り、特に、被管理装置においてポリシーの適用効果を評価し、この評価結果に基づいて、ポリシーをネットワークの利用状況に応じて動的に調整するようにしたポリシーベース管理システムの管理装置および被管理装置に関する。

## 【0002】

【従来の技術】 電子商取引や企業業務など、インターネットの商用化にともない、限られたネットワーク資源の40有効利用による利潤の最大化を図るために、ユーザやアプリケーションごとに所定の通信品質（QoS）を確保する必要性が高まっている。

【0003】 一方、このようなユーザやアプリケーションごとの通信品質を一元管理してネットワーク管理者の負担を軽減するために、ポリシーサーバにユーザやアプリケーションごとの通信品質をポリシー情報として登録し、散在するネットワーク機器にポリシーサーバからポリシー情報を配信して運用させるポリシーベース管理が普及している。このようなポリシーベース管理によれば、散在するネットワーク機器にポリシー情報を矛盾な

く設定できると共に、ポリシー情報の変更が容易になる。

【0004】IETF (Internet Engineering Task Force) で標準化が進められているインターネットの通信品質保証メカニズムの一つに、Differentiated Service (以下、DiffServと表現する) がある。ここでは、ユーザやアプリケーション毎にカスタマイズした通信品質を保証するためのポリシーが、ポリシーベース管理システムの管理装置から被管理装置へ配信されて運用される。

【0005】図8は、DiffServ対応ネットワークの構成を示した図であり、各トラフィックには、QoSを代表する識別子としてのPHB (per-hop behavior) が割り当てられる。各ルータ90は、入力されたトラフィックを前記PHBに応じたQoSで次のルータへ転送する。なお、各IPパケットには、前記PHBの代わりに6ビット長のDSCP (Differentiated Service Code Point: 通信品質情報) がDS (Differentiated Service) フィールドに割り当てられ、各ルータがPHBとDSCPとの対応付けを行う。

【0006】各ルータ90のインターフェース (I/F) は、送受信ノードに接続されるエッジI/F91と他のルータに接続されるコアI/F92とに区別される。前記エッジI/F91はさらに、送信ノードに接続されるイングレスI/F91 (in) と、受信ノードに接続されるエングレスI/F91 (en) とに区別される。エッジI/F91を備えたルータはエッジルータ90 (E) と呼ばれ、コアI/F92のみのルータはコアルータ90 (C) と呼ばれる。

【0007】上記したDiffServ対応ルータをはじめて通過するIPパケットは、送受信ノードのIPアドレスやポート番号の値に応じて、いくつかのQoSクラスに分類され、エッジルータ90 (E) において、そのDSCP値を割り当てられる。コアルータ90 (C) は、DSCPの値に基づいて各IPパケットを分類して通信品質制御を行い、次のルータへ転送する。DSCPの値はエッジルータ90 (E) のエングレスI/F91 (en) においてクリアされる。

【0008】IPパケットの分類にはクラッシファイア (classifier: 分類器) が用いられる。イングレスI/F91 (in) のクラッシファイアはMF (multi-field) クラッシファイアと呼ばれ、各IPパケットを、その送受信IPアドレス、送受信ポート番号、IPプロトコルバージョンの五のパラメータに基づいて分類する。コアI/F92のクラッシファイアはBA (Behavior Aggregate) クラッシファイアと呼ばれ、各IPパケットを前記DSCPの値で分類する。

【0009】

【発明が解決しようとする課題】ポリシーベースに基づくネットワーク管理では、ユーザ数やネットワークトラフィックの増大、あるいは新規アプリケーションの導入と

いった環境変化などにより、以前に配信したポリシーが何時までも有効に機能するとは限らない。このため、既設のポリシーに対して帯域が過剰に設定されるためにネットワーク資源が無駄に消費されたり、これとは逆に、ポリシーに対して帯域が過少に設定されるために所望のサービスを提供できない場合などが生じ得る。

【0010】したがって、ポリシーベースに基づくネットワーク管理では、(1) ポリシーの決定、(2) 決定されたポリシーの配信およびその運用、(3) 運用されている10 ポリシーの評価、(4) 評価結果に基づくポリシーの調整、を繰り返し実時間で行うことが望ましい。

【0011】これに対して、従来はネットワーク管理者がネットワーク上のトラヒックを常時監視し、既設のポリシーが実際のトラヒックに即していないと、その調整に必要な管理情報を別途に収集し、これに基づいてポリシーを再設定していた。しかしながら、ネットワーク環境は絶えず動的に変化するため、上記した調整方法では、ポリシーをネットワークの利用状況に応じて実時間で最適に調整することが困難であった。

【0012】20 本発明の目的は、上記した従来技術の課題を解決し、ネットワーク内の各ルータで運用されているポリシーを、トラヒックの状況に応じて実時間で最適に調整できるようにしたポリシーベース管理システムの管理装置および被管理装置を提供することにある。

【0013】

【課題を解決するための手段】上記した目的を達成するために、本発明は、ポリシー情報を管理装置で一元管理し、当該ポリシー情報を被管理装置へ配信してトラヒックを制御するポリシーベース管理システムの管理装置30 および被管理装置において、以下のような手段を講じた点に特徴がある。

【0014】(1) 管理装置に、ポリシー情報を入力するポリシー情報入力手段と、前記被管理装置においてポリシーの適用効果を評価させるための評価情報を入力するポリシー評価情報入力手段と、前記被管理装置で運用されるポリシーを、前記評価結果に基づいて被管理装置において動的に調整させるための調整情報を入力するポリシー調整情報入力手段と、前記入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報を前記被40 管理装置へ配信する配信手段とを設けた。

【0015】(2) 被管理装置に、管理装置から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段と、管理装置から配信されたポリシー評価情報に基づいて、運用中のポリシーを評価するポリシー評価手段と、管理装置から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを動的に調整するポリシー調整手段とを設けた。

【0016】上記した特徴によれば、各被管理装置に配信されて運用されているポリシーが、トラヒックの状況

に応じて動的に調整されるので、帯域などのネットワーク資源の過剰設定や過少設定が緩和されて、その有効利用が可能になる。

【0017】

【発明の実施の形態】以下、図面を参照して本発明を詳細に説明する。図1は、本発明を適用したポリシーベース管理システムの構成を示した機能ブロック図であり、ネットワークNT内でトラヒックを制御する被管理装置としての複数のルータ3と、ポリシー情報を記憶するポリシーサーバ1と、ポリシー情報を生成して各ルータ3へ配信する管理装置としてのネットワーク管理システム(NMS)2とを含む。

【0018】前記管理システム2は、各ルータ3において運用させるポリシーを入力するポリシー情報入力手段21と、各ルータ3において前記ポリシーの適用効果を評価するための評価情報を入力するポリシー評価情報入力手段22と、ルータ3で運用中のポリシーを前記評価結果に基づいて、当該ルータ3において動的に調整させるための調整情報を入力するポリシー調整情報入力手段23と、前記入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報が記述された管理スクリプトを各ルータ3へ配信する配信手段24とを含む。

【0019】前記ポリシー情報、ポリシー評価情報およびポリシー調整情報は、操作部および表示部等を含む適宜のマン・マシンI/F25を介してオペレータにより入力することができる。

【0020】前記各ルータ3は、前記管理システム2から配信されたポリシー情報を運用してトラヒックを制御するポリシー運用手段31と、前記管理システム2から配信されたポリシー評価情報に基づいて、運用中のポリシーの適用効果を評価するポリシー評価手段32と、前記管理システム2から配信されたポリシー調整情報および前記評価手段による評価結果に基づいて、運用中のポリシーを調整するポリシー調整手段33と、調整後のポリシー情報を他のルータ3へ、管理システム2を介して間接的に、あるいは管理システム2を介さずに直接的に通知する通知手段34とを含む。

【0021】図2は、前記ルータ3の主要部の構成を具体的に示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【0022】ポリシー運用手段31において、クラッシャイア3101は、入力I/F35を介して入力されたIPパケットを、その送信IPアドレス、受信IPアドレス、送信ポート番号、受信ポート番号およびIPプロトコルバージョンの5のパラメータに基づいて(MFクラッシャイアの場合)、あるいはDSCPの値に基づいて(BAクラッシャイアの場合)QoSクラスに分類する。

【0023】ミータ3102、3103、3104は、ポリシー情報で予め指定された転送レートやバーストサ

イズにトラヒックが適合するか否かを判断し、その結果に基づいて各トラヒックの出力先を切り替える。マーカ3105、3106は、DSCPの値を設定または置換して、当該トラフィック(またはパケット)のQoSクラスを変更する。マルチブレクサ3111、3112は、複数のトラヒックをマージする。

【0024】カウンタ3113～3117は、通過するIPパケット数やIPパケットバイト数をカウントする。無条件ドロップ3107は、パケットを無条件で破棄する。選択的ドロップ3108、3109、3110は、所定の条件に基づいてパケットを選択的に破棄する。キュー3118～3121は、入力されるIPパケットをキューイングする。スケジューラ3130は、前記各キュー3118～3121からIPパケットを所定の順序および優先度で読み出して出力I/F36へ出力する。

【0025】ポリシー評価手段32の監視機能部321は、各カウンタ3113～3117のカウント値に基づいて、破棄されたパケット数等を検知し、運用中のポリシーの適用効果を評価する。ポリシー調整手段33の制御機能部331は、前記ポリシー評価手段32による評価結果に基づいて、運用中のポリシーを適正に調整する。通知手段34の通知機能部341は、前記適用効果に関する評価結果を他のルータ3へ通知し、かつ他のルータから通知された評価結果をポリシー調整手段33の制御機能部331へ通知する。制御機能部331は、他のルータから評価結果を通知された場合も、前記と同様に、この評価結果に基づいてポリシーを適正に調整する。

【0026】次いで、上記した各ルータ3に対するポリシー情報、ポリシー評価情報およびポリシー調整情報の登録方法について説明する。

【0027】本実施形態では、4種類のポリシーA、B、C、Dを、オペレータが前記管理システム2のマン・マシンI/F25から登録するものとし、ポリシーA、B、Cの内容は図3に示した通りであるものとする。なお、ポリシーDは通信品質を保証しないベストエフォート(BE)なトラヒックとして扱い、各ポリシーA、B、Cのプロファイルは、図4に示した通りであるものとする。

【0028】図5、6、7は、管理システム2のマン・マシンI/F25の操作画面上に表示されるポリシー設定画面の一例を示した図であり、それぞれポリシーA、B、Cの入力例を示している。

【0029】ポリシー設定画面には、ポリシー情報を主に入力するポリシー情報入力領域51と、ポリシー評価情報を主に入力する閾値設定領域52と、ポリシー情報をルータ3において動的に調整させるためのポリシー調整情報を主に入力する自動制御設定領域53とが用意されている。

## 【0030】1. ポリシーAの設定(図5)

## ①ポリシー情報の入力

ポリシーAでは、図3に示したように、PHB(Expedited Forwarding Per-Hop-Behavior)がEF(Expedited Forwarding PHB: 遅延を許容しないQoS)なので、EFに対応するDSCP(Differentiated Service Code Point: 優先順位情報)の値“101110”をDSCPウインドウ511に登録する。

【0031】ポリシーAのプロファイル1では、図4に示したように、転送レート(Information Rate)閾値[Kbps]が“100”、バーストサイズ(Burst Size)閾値[Kbytes]が“20”なので、転送レート閾値ウインドウ512に“100”、バーストサイズ閾値ウインドウ513に“20”をそれぞれ登録する。

【0032】なお、“Single Rate Three Color Marker”や“Two Rate Three Color Marker”などを用いて、パケットがプロファイルに適合するか否かを決定する場合には、さらに適用チェックボックス514をチェックし、Committed InformationRateウインドウ515およびCommitted Burst Sizeウインドウ516に所望の値を設定する。

【0033】ここでは、図4に示したように、プロファイルを一つの組(転送レートおよびバーストサイズ)を使って決定する“単純トーカンパケット”を採用しているため、適用チェックボックス514をチェックすることなく、各ウインドウ515、516は未登録のまます。

【0034】DSCPの“In Profile”ウインドウ517には、プロファイルに適合するパケットのDSCP値を他のDSCP値に置換する際の値として“101110(EF)”を登録し、“Out Profile”ウインドウ518には、プロファイルに適合しないパケットのDSCP値を他のDSCP値に置換する際の値として“drop”すなわち“破棄”が登録される。

【0035】なお、先に述べた“Single Rate Three Color Marker”や“Two Rate Three Color Marker”において、半適合と判断されたパケットのDSCP値を他のDSCP値に置換する際の値は、“Indeterminate”ウインドウ519に登録することになる。

## 【0036】②ポリシー評価情報の入力

本実施形態では、運用されているポリシーの適用効果を評価するための情報として、受信パケット数、受信バイト数、廃棄パケット数などの各監視項目に関する閾値を、その監視周期と共に入力する。

【0037】ポリシーAでは、60秒当たりの廃棄パケット数が1000を超えると、閾値違反通知がポリシー調整手段33に対して発行されるものとし、“監視周期”ウインドウ521に60[秒]、“破棄パケット数”ウインドウ522に“1000以上”が登録される。したがって、ポリシーAでは、60秒間における廃棄パケッ

ト数が1000を超えると、ポリシー調整手段33によるポリシーの自動調整が開始されることになる。

【0038】なお、複数の監視項目の閾値が同時に指定されている場合には、少なくとも一つの監視項目の閾値が超えた場合に通知するが、全ての監視項目の閾値が超えた場合のみ通知したり、これらの監視項目からなる論理条件式を定義して通知を発行させることも可能である。

## 【0039】③ポリシー調整情報の入力

10 本実施形態では、前記閾値違反が通知された場合のみならず、閾値違反が通知されない場合であっても、所定の制御周期ごとに前記ポリシーの適用効果を評価してポリシーを自動調整するようにしている。

【0040】すなわち、本実施形態では、各60秒間の破棄パケット数が1000を越えない限りは閾値違反とならないが、例えば60秒間の破棄パケット数が500程度であっても、これを救うためにはポリシーとして設定する帯域などのネットワーク資源を増やすことが望ましい。これとは逆に、破棄パケット数が0の場合には、

20 ポリシーが品質過剰と予測されるので、当該ポリシーの品質を下げることが望ましい。

【0041】そこで、本実施形態では所定の制御周期を設定し、当該制御周期内でのトラヒックに応じてポリシーを動的に調整するために、ネットワークの利用状況に応じた実時間でポリシーの調整を行う制御周期、調整後のポリシーAに割り当てる転送レート、バーストサイズおよび置換するDSCP値を指定する。

【0042】図5の例では、現在の転送レート閾値(100)およびバーストサイズ閾値(20)を、直前の130 2時間以内に監視された最大転送レートの1.1倍ならびに最大バーストサイズの1.0倍の値に調整するものとし、制御周期の時間ウインドウ531に“12”[時間]、Peak Information Rateウインドウ532に“1.1”倍、Peak Burst Sizeウインドウ533に“1.0”倍が、それぞれ設定される。

【0043】したがって、本実施形態のポリシーAでは、閾値違反が発生しない場合であっても、転送レート閾値およびバーストサイズ閾値が、12時間ごとにネットワークの利用状況に応じて動的に調整されるようになる。

【0044】以上のようにして、各情報の設定を終了すると、“確認ボタン”を押下して当該入力操作を終了する。配信手段24は、入力された各情報を各ルータ3へ配信する。

## 【0045】2. ポリシーBの設定(図6)

## ①ポリシー情報の入力

ポリシーBでは、図3に示したように、PHBがAF11(Assured Forwarding Group: エンド・ツー・エンドでの許容パケット紛失率を小さくする)なので、AF11に対応するDSCPの値“001010”をDSCP

ウインドウ 511 に登録する。

【0046】ポリシーBのプロファイル2では、図4に示したように、転送レート閾値 (Information Rate)

[Kbps] が “100”、バーストサイズ閾値 (Burst Size) [Kbytes] が “100” なので、転送レート閾値ウインドウ 512 に 100、バーストサイズ閾値ウインドウ 513 に “100” を、それぞれ登録する。なお、Committed Information Rate および Committed Burst Size の指定は前記と同様とする。

【0047】DSCP の “In Profile” ウインドウ 517 には、プロファイルに適合するパケットの DSCP 値を他の DSCP 値に置換する際の値として “001010” (AF11) を登録し、 “Out Profile” ウインドウ 518 には、プロファイルに適合しないパケットの DSCP 値を他の DSCP 値に置換する際の値として “001100” (AF12) が登録される。

【0048】すなわち、本実施形態のポリシーBでは、プロファイルに適合するパケットの DSCP 値は変更せず、適合しないパケットは、その DSCP 値が “001100 (AF12)” に更新されて送信優先度を下げる。

【0049】②ポリシー評価情報の入力

ポリシーA と同様なので、その説明は省略する。

【0050】③ポリシー調整情報の入力

本実施形態では、制御周期の 12 時間以内に閾値違反が検知されている場合 (Over) は、前記転送レート閾値 (ここでは、100Kbps) を越えていない (In Profile) パケットの DSCP 値を “001100 (AF12)” に置換して送信優先度を下げる調整を行う。したがって、 “DSCP” のチェックボックス 535 をチェックし、 “In Profile” ウインドウ 536 に “001100” (AF12) を登録する。

【0051】なお、図6では未記入であるが、制御周期の 12 時間以内に閾値違反が検知されていない場合の調整値は、 “Under” 以下の各欄に登録する。

【0052】3. ポリシーCの設定 (図7)

①ポリシー情報の入力

ポリシーCでは、図3に示したように、PHB が AF12 (AF11 よりも優先度が低い) なので、AF12 に対応する DSCP の値 “001100” を DSCP ウインドウ 511 に登録する。

【0053】ポリシーCのプロファイル3では、図4に示したように、転送レート閾値 (Information Rate)

[Kbps] が “200”、バーストサイズ閾値 (Burst Size) [Kbytes] が “100” なので、転送レート閾値ウインドウ 512 に 200、バーストサイズ閾値ウインドウ 513 に “100” をそれぞれ登録する。なお、Committed Information Rate および Committed Burst Size の指定は前記と同様とする。

【0054】DSCP の “In Profile” ウインドウ 51

7 には、プロファイルに適合するパケットの DSCP 値を他の DSCP 値に置換する際の値として “001100” (AF12) を登録し、 “Out Profile” ウインドウ 518 には、プロファイルに適合しないパケットの DSCP 値を他の DSCP 値に置換する際の値として “000000” (BE: Best Effort) が登録される。

【0055】すなわち、本実施形態のポリシーCでは、プロファイルに適合するパケットの DSCP 値は変更せず、適合しないパケットは、帯域制御や優先制御をまったく行わない通常のインターネットのトラフィックとして扱うように調整する。

【0056】②ポリシー評価情報の入力

ポリシーA、B と同様なので、その説明は省略する。

【0057】③ポリシー調整情報の入力

本実施形態では、制御周期の 12 時間以内に閾値違反が検知されている場合 (Over) は、前記転送レート閾値 (ここでは、200Kbps) を越えていない (In Profile) パケットの DSCP 値を “000000 (BE)” に変更して優先制御の対象外とする。これとは逆に、制御周期の 12 時間以内に閾値違反が検知されていない場合 (Under) には、プロファイルに適合 (In Profile) するパケットの DSCP 値を “001010” (AF11) に変更して送信優先度を上げる調整を行う。

【0058】したがって、 “DSCP” のチェックボックス 535 をチェックし、 “Over” の “In Profile” ウインドウ 536 に “000000” (BE) を登録し、 “Under” の “In Profile” ウインドウ 537 に “001010” (AF11) を登録する。

【0059】4. ポリシーDの決定

30 ポリシーA、B、C で決定した以外の DSCP を持つパケットは、従来のインターネットと同様に、すべてベストエフォートなトラフィックとして扱う。以降、これをポリシーD と表現する。

【0060】以上のようにして入力されたポリシー情報、ポリシー評価情報およびポリシー調整情報は、管理システム 2 の配信手段 24 により、例えば COPS (Common Open Policy Service)、SNMP (Simple Network Management Protocol)、または CLI (Command Line Interface) 等のプロトコルを用いて各ルータ 3 へ配信される。

【0061】各ルータ 3 では、ポリシー情報がポリシー運用手段 31 において各ミータ 3102、3103、3104 および各マルチブレクサ 3105、3106 に登録され、ポリシー評価情報がポリシー評価手段 32 に登録され、ポリシー調整情報はポリシー調整手段 33 に登録される。

【0062】以上のようにして、各情報の設定が終了し、ポリシー運用手段 31 においてポリシーが運用されると、ポリシー A を適用されるパケットは、クラッシャイア 3101 からミータ 3102 へ配信される。ミー

タ3102は、入力されたパケットの転送レートが100 [Kbps] を越えず、かつバーストサイズが20 [Kbytes] を越えない限りは、入力されたパケットを全てキュー3118へ転送する。キュー3118に蓄積されたパケットは、スケジューラ3130により読み出され、出力通信I/F36を介して次段へ転送される。

【0063】これに対して、転送レートが100 [Kbps] を越えるか、あるいはバーストサイズが20 [Kbytes] を越えると、前記ミータ3102は、超えた分のパケットをカウンタ3113へ配信する。カウンタ3113でカウントされたパケットは、無条件ドロッパ3107において全て破棄される。

【0064】ポリシーBを適用されるパケットは、クラッシファイア3101からミータ3103へ配信される。ミータ3103では、入力されたパケットの転送レートが100 [Kbps] を越えず、かつバーストサイズが100 [Kbytes] を越えない限りはマルチブレクサ3111へ配信し、それ以外であればマーカ3105へ配信する。マーカ3105は、そのパケットのDSに登録されたDSCP値(001010)を(001100)に変換して、その優先順位を下げる。

【0065】マルチブレクサ3111は、前記ミータ3103およびマーカ3105から配信されたパケットを結合し、カウンタ3114を介してドロッパ3108へ転送する。前記ドロッパ3108は、キュー長が所定値よりも長くなると、それ以上のパケットを破棄する。ドロッパ3108で破棄されなかったパケットは、カウンタ3115を介してキュー3118へ転送される。前記カウンタ3114、カウンタ3115はドロッパ3108の前後でパケット数をカウントするので、両者のカウント値の差分が前記ドロッパ3108で破棄されたパケット数となる。

【0066】ポリシーCについては、ドロッパ3109の構成が前記ポリシーBのドロッパ3108と異なり、ポリシーCのドロッパ3109では前記ドロッパ3108よりも多くのパケットを破棄するのみで、それ以外の動作は同様なので、その説明を省略する。

【0067】ポリシーDを適用されるパケットは、クラッシファイア3101からドロッパ3110へ配信される。ドロッパ3110は、そのキュー長が所定値よりも長くなると、それ以上のパケットを破棄し、それ以外のパケットをキュー3121へ出力する。

【0068】以上のようにして各ポリシーが運用されると、監視機能部321は、各カウンタのカウント値を、前記指定された監視周期で検知して破棄パケット数を算出し、算出結果に基づいて各ポリシーの適用効果を評価する。

【0069】ここで、例えばポリシーAが適用されて破棄されたパケット数をカウントするカウンタ3113のカウント値が“1000”を越えると、これを制御機能

部331へ通知してポリシーの調整を指示すと共に、通知機能部341を介して他のルータの制御機能部331へも指示する。

【0070】制御機能部331は、ミータ3102に既登録の設定値、すなわち転送レート閾値の100 [Kbps] 、バーストサイズ閾値の20 [Kbytes] を、この12時間以内に検知された転送レートおよびバーストサイズの1.1倍、1.0倍にそれぞれ設定する。

【0071】ここで、破棄パケットが検知されているということは、100 [Kbps] 以上の転送レートおよび/または20 [Kbytes] 以上のバーストサイズが検知されているはずである。したがって、前記転送レート閾値および/またはバーストサイズ閾値には、それまでよりも大きな値が設定されることになるので、ポリシーの品質が向上することになる。

【0072】前記監視機能部321はさらに、閾値違反が発生しない場合であっても、前記指定された監視周期(本実施形態では、いすれのポリシーでも“12”時間)ごとに、制御機能部331に対して自動制御を指示する。

【0073】制御機能部331は、ミータ3102に既登録の設定値、すなわち転送レート閾値の100 [Kbps] 、バーストサイズ閾値の20 [Kbytes] を、この12時間以内に検知された帯域およびバーストサイズの1.1倍、1.0倍にそれぞれ設定する。

【0074】このとき、破棄パケットが少しでも検知されている状況下では、100 [Kbps] 以上の転送レートおよび/または20 [Kbytes] 以上のバーストサイズが検知されているはずである。したがって、前記転送レート閾値および/またはバーストサイズ閾値には、それまでよりも大きな値が設定されるので、ポリシーの品質が向上し、品質不足が緩和されることになる。

【0075】これに対して、破棄パケットが検知されていなければ、100 [Kbps] 以上の転送レートおよび20 [Kbytes] 以上のバーストサイズが検知されていないので、前記転送レート閾値およびバーストサイズ閾値には、それまでよりも小さな値が設定されることになる。したがって、ポリシーの品質が現在よりも低下して品質過剰が緩和されることになる。

【0076】なお、他のポリシーB、C、Dの動作は、上記したポリシーAに関する動作説明から明らかなので、その説明は省略する。

【0077】上記した実施形態では、本発明をDiffServへ適用した場合を例にして説明したが、本発明はこれのみに限定されるものではなく、IETFやDMTFが標準化を積極的に進めている“Integrated Service”(通称Intserv)にも同様に適用することができる。また、主にパケットの送信優先制御や帯域制御を行うポリシーベース管理のみならず、ユーザや会社組織、ホストや端末、ならびにアプリケーションごとにカスタマイズした

アクセス制御を行うファイアウォールを用いたポリシー・ベースのネットワーク管理にも、同様に適用できる。

【0078】

【発明の効果】本発明によれば、以下のような効果が達成される。

【0079】(1) 各被管理装置（ルータ）に配信されて運用されているポリシーが、トラヒックの状況に応じて動的に調整されるので、通信品質の過剰や不足が緩和されてネットワーク資源の有効利用が可能になる。

【0080】(2) 一つの被管理装置におけるポリシーの調整内容が他の被管理装置にも反映されるので、ポリシー調整の実効が得られる。

【図面の簡単な説明】

【図1】 本発明を適用したポリシーベース管理システムの構成を示した機能ブロック図である。

【図2】 被管理装置としてのルータの主要部の構成を示したブロック図である。

【図3】 各ポリシーA, B, Cの内容を模式的に表現

した図である。

【図4】 各プロファイルの内容を模式的に表現した図である。

【図5】 ポリシーAを設定する際のポリシー入力画面の表示例を示した図である。

【図6】 ポリシーBを設定する際のポリシー入力画面の表示例を示した図である。

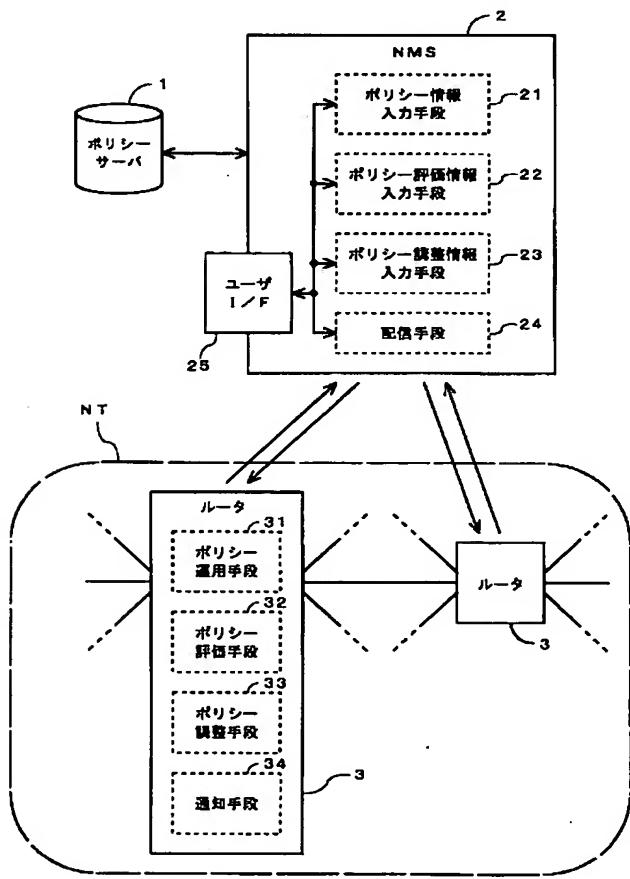
【図7】 ポリシーCを設定する際のポリシー入力画面の表示例を示した図である。

【図8】 DiffServ対応ネットワークの構成を示した図である。

【符号の説明】

ポリシーサーバ 1 …, 2 …ネットワーク管理システム, 3 …ルータ, 21 …ポリシー情報入力手段, 22 …ポリシー評価情報入力手段, 23 …ポリシー調整情報入力手段, 24 …配信手段, 25 …マン・マシン I/F, 31 …ポリシー運用手段, 32 …ポリシー評価手段, 33 …ポリシー調整手段, 34 …通知手段

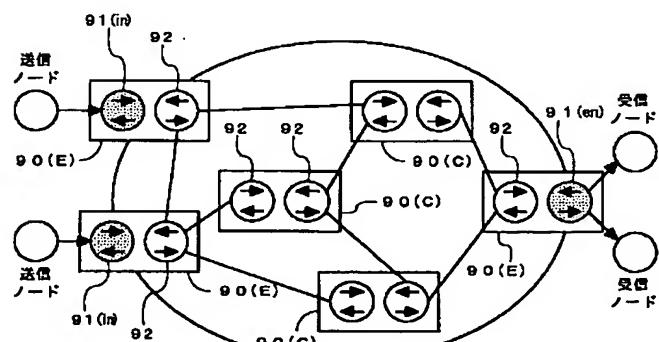
【図1】



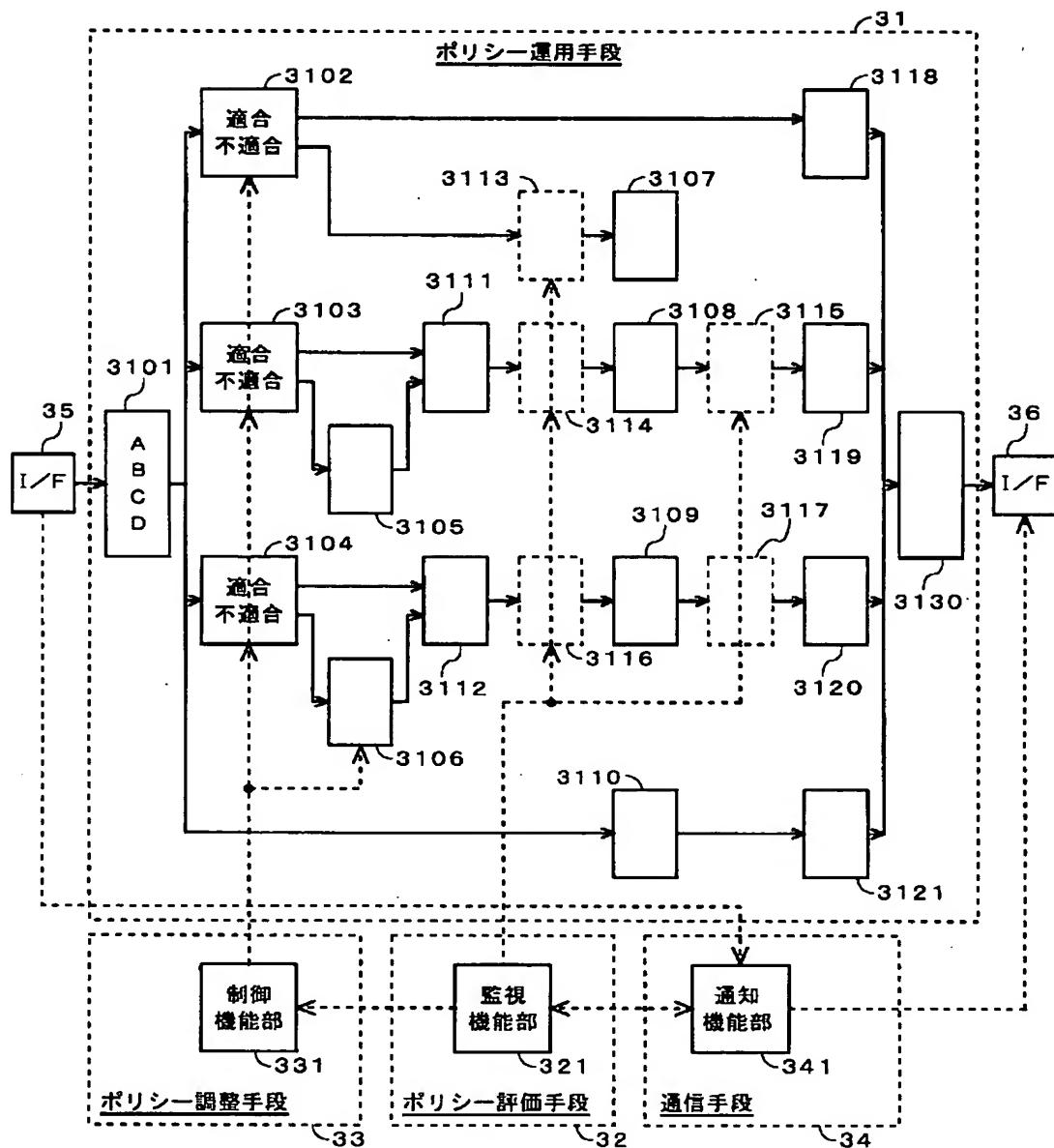
【図3】

ポリシーID	DSCP	PHB	プロファイル	制御方法
A	101110	E F	Profile1	プロファイルに適合しないものを破棄。
B	001010	A F11	Profile2	プロファイルに適合しないものをマーキング。キューが溢れた場合、キューの最後のパケットを破棄。
C	001100	A F12	Profile3	プロファイルに適合しないものをマーキング。キューが溢れた場合、キューの最後のパケットを破棄。

【図8】



【図2】



【図4】

	Type	転送レート (Kbps)	バーストサイズ (Kbytes)
Profile1	単純トーケンパケット	100	20
Profile2	単純トーケンパケット	100	100
Profile3	単純トーケンパケット	200	100

【図 5】

ポリシー ID A

BA Classifier

DSCP 101110(E F) □

Meter

Information Rate (Kbps) 100  
Burst Size (Kbytes) 20

適用 613

Committed Information Rate (Kbps) 615  
Committed Peak Burst Size (Kbytes) 616

DSCP 617

In Profile 101110(E F) □  
Indeterminate □  
Out Profile drop □

監視設定 621

監視周期 60 秒 □  
バイト数 □ 帯域借用回数 □  
パケット数 □ overaction回数 □  
破棄パケット数 □ 1000 average idle □  
overlimitパケット数 □ undertime □  
overlimit回数 □ 622

自動制御設定 631

制御周期  帯域 632

分 Peak Information Rate (Kbps) 1.1倍 Over  
1.2 時間 Committed Information Rate (Kbps) 633倍 In Profile □  
 日 Indeterminate □  
 週間 Out Profile □

制御周期  帯域 635

分 Peak Information Rate (Kbps) 636倍 Over  
1.2 時間 Committed Information Rate (Kbps) 636倍 In Profile 001100(A F12) □  
 日 Indeterminate □  
 週間 Out Profile □

バーストサイズ 633 Under

Peak Burst Size (Kbytes) 1.0倍 In Profile □  
Committed Burst Size (Kbytes) 634倍 Indeterminate □  
Out Profile □

確定 534 閉じる

【図 6】

ポリシー ID B

BA Classifier

DSCP 001010(A F11) □

Meter

Information Rate (Kbps) 100  
Burst Size (Kbytes) 100

適用 613

Committed Information Rate (Kbps) 615  
Committed Peak Burst Size (Kbytes) 616

DSCP 617

In Profile 001010(A F11) □  
Indeterminate □  
Out Profile 001100(A F12) □

監視設定 621

監視周期 60 秒 □  
バイト数 □ 帯域借用回数 □  
パケット数 □ overaction回数 □  
破棄パケット数 □ 1000 average idle □  
overlimitパケット数 □ undertime □  
overlimit回数 □ 622

自動制御設定 631

制御周期  帯域 632

分 Peak Information Rate (Kbps) 1.1倍 Over  
1.2 時間 Committed Information Rate (Kbps) 633倍 In Profile □  
 日 Indeterminate □  
 週間 Out Profile □

制御周期  帯域 635

分 Peak Information Rate (Kbps) 636倍 Over  
1.2 時間 Committed Information Rate (Kbps) 636倍 In Profile 001100(A F12) □  
 日 Indeterminate □  
 週間 Out Profile □

バーストサイズ 633 Under

Peak Burst Size (Kbytes) 1.0倍 In Profile □  
Committed Burst Size (Kbytes) 634倍 Indeterminate □  
Out Profile □

確定 534 閉じる

【図 7】

ポリシーID C

BA Classifier

DSCP 001100(A F12) ▽ 511

Meter

Information Rate (Kbps) 200 512

Burst Size (Kbytes) 100

適用 513

Committed Information Rate (Kbps) 514

Committed Peak Burst Size (Kbytes) 515

DSCP 517

In Profile 001100(A F12) ▽ 516

Indeterminate ▽ 517

Out Profile 000000(B E) ▽ 518

監査設定 52

監査周期 60 秒 ▽

バイト数  [ ] 希域借用回数  [ ]

パケット数  [ ] overaction回数  [ ]

確実パケット数  [ ] 1000 average idle  [ ]

overlimitパケット数  [ ] undertime  [ ]

overlimit回数  [ ]

自動制御設定 531 53

制御周期  希域 535 DSCP Over

分 Peak Information Rate (Kbps)  倍 In Profile 000000(B E) ▽ 536

時間 12 時間 Committed Information Rate(Kbps)  倍 Indeterminate ▽

日  Out Profile ▽

過間  パーブルサイズ Under 537

Peak Burst Size (Kbytes)  倍 In Profile 001010(A F11) ▽ 538

Committed Burst Size (Kbytes)  倍 Indeterminate ▽

Out Profile ▽

確定 閉じる